THE FIELDS OF DEFINITION OF BRANCHED GALOIS COVERS OF THE PROJECTIVE LINE

HILAF HASSON

Abstract. In this paper I explore the structure of the fields of definition of Galois branched covers of the projective line over $\bar{\mathbb{Q}}$. The first main result states that every mere cover model has a unique minimal field of definition where its automorphisms are defined, and goes on to describe special properties of this field. One corollary of this result is that for every G-Galois branched cover there is a field of definition which is Galois over its field of moduli, with Galois group a subgroup of $\mathrm{Aut}(G)$. The second main theorem states that the field resulting by adjoining to the field of moduli all of the roots of unity whose order divides some power of $|Z(G)|$ is a field of definition. By combining this result with results from an earlier paper, I prove corollaries related to the Inverse Galois Problem. For example, it allows me to prove that for every finite group G, there is an extension of number fields $\mathbb{Q} \subset E \subset F$ such that F/E is G-Galois, and $E/\mathbb{Q}$ ramifies only over those primes that divide $|G|$. I.e., G is realizable over a field that is "close" to $\mathbb{Q}$.

1. Overview

The Inverse Galois Problem asks whether every finite group G is realizable as a Galois group over $\mathbb{Q}$ (or more generally over every number field K). Most attempts to solve the Inverse Galois Problem over a number field K have focused on trying to solve its geometric analogue, the Regular Inverse Galois Problem. The Regular Inverse Galois Problem asks whether for every finite group G there is a G-Galois branched cover of the projective line over $\bar{\mathbb{Q}}$ that is defined (together with its automorphisms) by polynomials with coefficients in K. It is well known that for every finite group G there is a G-Galois branched cover of the projective line over $\bar{\mathbb{Q}}$. (This is proven via transcendental methods; see Remark 2.4 for more details.) While most previous work has focused on the field of moduli (see Definition 2.5) of such covers, the focus of this paper is on the structure of their fields of definition.

In Section 2 we provide an introduction to the definitions and concepts in this paper. In Section 3 we give a bijection between mere cover models and a group-theoretic object. (See Lemma 3.1.) This allows us to prove the first main theorem of this paper in Section 4, namely Theorem 4.3. This theorem states that every mere cover model of a G-Galois branched cover has a unique minimal field where its automorphisms are defined, and this field of definition has special properties. This theorem has several noteworthy corollaries. Among them, it follows that for every G-Galois branched cover of $\mathbb{P}^1_{\bar{\mathbb{Q}}}$ there is a field of definition that is Galois over the field of moduli, with Galois group a subgroup of $\mathrm{Aut}(G)$. (See Corollary 4.5.) In particular, there is always a "small" field of definition over the field of moduli. Finally, in Section 5 we construct a special field of definition (infinite over the field of moduli) for every G-Galois branched cover, resulting from adjoining certain elements to the field of moduli. (See Theorem 5.1.) This, together with results from a previous paper ([10]), allow us to prove several corollaries (gathered in Corollary 5.2). For example, it allows us to prove that for every finite group G, there is an extension of number fields $\mathbb{Q} \subset E \subset F$ such that F/E is G-Galois, and $E/\mathbb{Q}$ ramifies only over those primes that divide $|G|$. I.e., G is realizable over a field that is "close" to $\mathbb{Q}$.

Date: January 19, 2013.

This paper is based in large part on portions of the author's doctoral thesis, written at the University of Pennsylvania under the supervision of David Harbater.

2. Introduction and Definitions

Notation 2.1. Given an integral scheme S, we write $\kappa(S)$ for its function field.

Definition 2.2. Let K be a field, and let X_K and Y_K be connected, normal, complete curves over K. We say that a map $X_K \to Y_K$ of K-curves is a *branched cover* (or simply a cover) if the map is finite and generically étale. We say that a branched cover is *Galois* if the induced extension of function fields $\kappa(X_K)/\kappa(Y_K)$ is a Galois extension of fields. We sometimes refer to branched covers as *mere covers*.

Let G be a finite group. A *G-Galois branched cover* is a branched cover $X_K \to Y_K$ which is Galois, together with an isomorphism of $\mathrm{Gal}(\kappa(X_K)/\kappa(Y_K))$ with G.

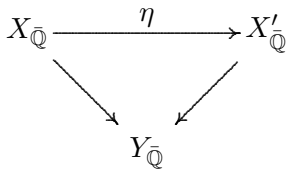
Definition 2.3. Let G be a finite group, and let $X_{\bar{\mathbb{Q}}} \to Y_{\bar{\mathbb{Q}}}$ be a G-Galois branched cover of curves over $\bar{\mathbb{Q}}$. We say that $K \subset \bar{\mathbb{Q}}$ is a *field of definition of $X_{\bar{\mathbb{Q}}} \to Y_{\bar{\mathbb{Q}}}$ as a mere cover* if it descends to a map of K-curves $X_K \to Y_K$. (Any such $X_K \to Y_K$ is called a K-model of $X_{\bar{\mathbb{Q}}} \to Y_{\bar{\mathbb{Q}}}$.) We say that K is a *field of definition as a G-Galois branched cover* if $X_{\bar{\mathbb{Q}}} \to Y_{\bar{\mathbb{Q}}}$ has a K-model that is Galois.

Let G be a finite group. In this paper we will be interested in G-Galois branched covers $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ of the projective line. Such covers have a special importance in Galois Theory. Namely, if a number field K is a field of definition of $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ as a G-Galois branched cover then Hilbert's Irreducibility Theorem ([8], Chapter 11) implies that G is the Galois group of a Galois field extension of K. In particular, if for every finite group G there is a G-Galois branched cover $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ that descends to $\mathbb{Q}$ (as a G-Galois branched cover) then the answer to the Inverse Galois Problem is affirmative.

Remark 2.4. Let $a_1, ..., a_r$ be closed points of $\mathbb{P}^1_{\mathbb{C}}$. Riemann's Existence Theorem (see [9], exposé XII) states that every topological covering space of $\mathbb{P}^1_{\mathbb{C}} \smallsetminus \{a_1, ..., a_r\}$ is defined by polynomials. It follows that there is an equivalence of categories between G-Galois branched covers of $\mathbb{P}^1_{\mathbb{C}} \smallsetminus \{a_1, ..., a_r\}$ that are étale and principal G-bundles of the induced topological space. Since the (topological) fundamental group of the Riemann Sphere punctured at r points is free with $r-1$ generators, it follows that it has a principal G-bundle for every finite group G that is generated by $r-1$ elements. In particular it implies that for every finite group G there exists a G-Galois branched cover of $\mathbb{P}^1_{\mathbb{C}}$. In fact, if we choose $a_1, ..., a_r$ so that they come from closed points of $\mathbb{P}^1_{\bar{\mathbb{Q}}}$ it follows from an argument of Grothendieck that the cover descends to $\bar{\mathbb{Q}}$. Therefore, for every finite group G there exists a G-Galois branched cover of $\mathbb{P}^1_{\bar{\mathbb{Q}}}$. However, since the proof of Riemann's Existence Theorem is not constructive, very little is known about the fields of definition of these covers.

Previous work on the structure of fields of definition of G-Galois branched covers (resp. mere covers) has concentrated on the "field of moduli". The field of moduli is a field naturally associated to a G-Galois branched cover (resp. mere cover), and is the best candidate for the smallest field of definition (if one exists).

Definition 2.5. Let G be a finite group, and let $X_{\bar{\mathbb{Q}}} \to Y_{\bar{\mathbb{Q}}}$ and $X'_{\bar{\mathbb{Q}}} \to Y_{\bar{\mathbb{Q}}}$ be G-Galois branched covers of $Y_{\bar{\mathbb{Q}}}$. We say that they are *isomorphic as mere covers* if there exists an isomorphism η that makes the following commute:



If η commutes with the given isomorphisms of $\mathrm{Gal}(\kappa(X_{\bar{\mathbb{Q}}})/\kappa(Y_{\bar{\mathbb{Q}}}))$ and $\mathrm{Gal}(\kappa(X'_{\bar{\mathbb{Q}}})/\kappa(Y_{\bar{\mathbb{Q}}}))$ with G, we say that $X_{\bar{\mathbb{Q}}} \to Y_{\bar{\mathbb{Q}}}$ and $X'_{\bar{\mathbb{Q}}} \to Y_{\bar{\mathbb{Q}}}$ are *isomorphic as G-Galois branched covers*.

Let $X_{\bar{\mathbb{Q}}} \to Y_{\bar{\mathbb{Q}}}$ be a G-Galois branched cover of curves over a field $\bar{\mathbb{Q}}$. Let K be a subfield of $\bar{\mathbb{Q}}$. The *field of moduli* of $X_{\bar{\mathbb{Q}}} \to Y_{\bar{\mathbb{Q}}}$ as a G-Galois branched cover (resp. mere cover) relative to K is the subfield of $\bar{\mathbb{Q}}$ fixed by those automorphisms of $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$ that take the G-Galois branched cover (resp. mere cover) to an isomorphic copy of itself. We will use the convention that the field of moduli is always taken relative to $\mathbb{Q}$, unless otherwise stated.

Let G be a finite group, and let $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ be a G-Galois branched cover. It is clear that the field of moduli of $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ as a G-Galois branched cover (resp. mere cover) is contained in all of its fields of definition as a G-Galois branched cover (resp. mere cover).

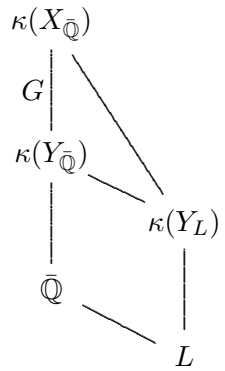
David Harbater and Kevin Coombes have proven in [3] that the field of moduli of $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$, considered as a G-Galois branched cover (resp. mere cover) is in fact equal to the intersection of all of its fields of definition as a G-Galois branched cover (resp. mere cover). Furthermore, the field of moduli of $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ as a mere cover is a field of definition as a mere cover, and therefore the unique minimal field of definition as a mere cover.

It is important to note that the field of moduli of a G-Galois branched cover of the projective line is not necessarily a field of definition as a G-Galois branched cover. In other words, a G-Galois branched cover may not have a *unique* minimal field of definition. The obstruction for the field of moduli M of a G-Galois branched cover to being a field of definition (as a G-Galois branched cover) lies in $H^2(M, Z(G))$. (See [2], [7] and [5]. The reader may also wish to consult [6].) In particular, if G is centerless or if M has cohomological dimension 1 it follows that the field of moduli is a field of definition. In [13] Stefan Wewers has explored this obstruction in detail.

3. Mere Cover Models and Sections

Let G be a finite group, and let $X_{\bar{\mathbb{Q}}} \to Y_{\bar{\mathbb{Q}}}$ a G-Galois branched cover of normal complete curves over $\bar{\mathbb{Q}}$. Let L be a field of definition of $X_{\bar{\mathbb{Q}}} \to Y_{\bar{\mathbb{Q}}}$ as a mere cover, and let Y_L be an L-model of $Y_{\bar{\mathbb{Q}}}$. Let Ω be the set of mere cover models $X_L \to Y_L$ of $X_{\bar{\mathbb{Q}}} \to Y_{\bar{\mathbb{Q}}}$ over L that lie above Y_L. The goal of this section is to give a bijection between Ω and the set of sections of some epimorphism of pro-finite groups. In order to do that, we require some notation.

We have following diagram of fields:



Since we assumed L is a field of definition as a mere cover, Lemma 2.4 in [1] (see also [11]) implies that $\kappa(X_{\bar{\mathbb{Q}}})$ is Galois over $\kappa(Y_L)$.

We have a short exact sequence:

$$1 \to G \to \mathrm{Gal}(\kappa(X_{\bar{\mathbb{Q}}})/\kappa(Y_L)) \to \mathrm{Gal}(\kappa(Y_{\bar{\mathbb{Q}}})/\kappa(Y_L)) \to 1$$

Let $\mathrm{Gal}(L)$ denote the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/L)$. Let $f : \mathrm{Gal}(\kappa(X_{\bar{\mathbb{Q}}})/\kappa(Y_L)) \twoheadrightarrow \mathrm{Gal}(L)$ be the composition of the quotient map $\mathrm{Gal}(\kappa(X_{\bar{\mathbb{Q}}})/\kappa(Y_L)) \twoheadrightarrow \mathrm{Gal}(\kappa(Y_{\bar{\mathbb{Q}}})/\kappa(Y_L))$ with the isomorphism $\mathrm{Gal}(\kappa(Y_{\bar{\mathbb{Q}}})/\kappa(Y_L)) \xrightarrow{\sim} \mathrm{Gal}(L)$. In other words, the map f takes an automorphism σ in $\mathrm{Gal}(\kappa(X_{\bar{\mathbb{Q}}})/\kappa(Y_L))$ to the restriction $\sigma|_{\bar{\mathbb{Q}}}$ of σ to $\bar{\mathbb{Q}}$. We get the following short exact sequence.

$$1 \to G \to \mathrm{Gal}(\kappa(X_{\bar{\mathbb{Q}}})/\kappa(Y_L)) \xrightarrow{f} \mathrm{Gal}(L) \to 1$$

Let $\mathrm{Sec}(f)$ denote the set of sections of f in the category of pro-finite groups.

Let $X_L \to Y_L$ in Ω be a mere cover model of $X_{\bar{\mathbb{Q}}} \to Y_{\bar{\mathbb{Q}}}$. Note that $\kappa(X_{\bar{\mathbb{Q}}})$ is naturally isomorphic to the tensor product $\bar{\mathbb{Q}} \otimes_L \kappa(X_L)$. We denote by $\omega_{X_L/Y_L} : \mathrm{Gal}(L) \to \mathrm{Gal}(\kappa(X_{\bar{\mathbb{Q}}})/\kappa(Y_L))$ the map taking σ to $\sigma \otimes \mathrm{id}_{\kappa(X_L)}$.

Lemma 3.1. *In the above situation, the following hold:*

1. *Let $\alpha : \Omega \to \mathrm{Sec}(f)$ be the map taking a mere cover model $X_L \to Y_L$ to ω_{X_L/Y_L}. Then α is a bijection.*
2. *Let $X_L \to Y_L$ be a mere cover model of $X_{\bar{\mathbb{Q}}} \to Y_{\bar{\mathbb{Q}}}$. Then $X_L \to Y_L$ is Galois if and only if the image of w_{X_L/Y_L} commutes with G.*

Proof. In order to prove that α is onto, we first prove that for every section $s \in \mathrm{Sec}(f)$, the field L is algebraically closed in $\kappa(X_{\bar{\mathbb{Q}}})^{s(\mathrm{Gal}(L))}$. It is straightforward to see that the natural map $\mathrm{Ker}(f) \to \mathrm{Gal}(\kappa(X_{\bar{\mathbb{Q}}})/\kappa(Y_L))/s(Gal(L))$ is a bijection of sets. Therefore the field $\kappa(X_{\bar{\mathbb{Q}}})^{s(\mathrm{Gal}(L))}$ has degree $|\mathrm{Ker}(f)| = |G|$ over $\kappa(Y_L)$. This implies that $\kappa(Y_{\bar{\mathbb{Q}}})$ is linearly disjoint from $\kappa(X_{\bar{\mathbb{Q}}})^{s(\mathrm{Gal}(L))}$ over $\kappa(Y_L)$, and therefore L is algebraically closed in $\kappa(X_{\bar{\mathbb{Q}}})^{s(\mathrm{Gal}(L))}$.

It follows from the above that there is a mere cover model $X_{L,s} \to Y_L$ that induces the field extension $\kappa(X_{\bar{\mathbb{Q}}})^{s(\mathrm{Gal}(L))}/\kappa(Y_L)$, and that the field $\kappa(X_{\bar{\mathbb{Q}}})$ is equal to the the compositum $\bar{\mathbb{Q}}\cdot\kappa(X_{L,s})$. Let σ be an element of $\mathrm{Gal}(L)$. Since both $s(\sigma)$ and $w_{X_{L,s}/Y_L}(\sigma)$ restrict to σ on $\bar{\mathbb{Q}}$, and restrict to the trivial automorphism on $\kappa(X_{L,s})$, it follows that $s(\sigma)$ is equal to $w_{X_{L,s}/Y_L}(\sigma)$. In other words, α is onto.

In order to finish the proof of Claim (1) of this lemma, it remains to prove that α is injective. Let $X_L \to Y_L$ be an element of Ω. As we have seen above, the field extension $\kappa(X_{\bar{\mathbb{Q}}})^{w_{X_L/Y_L}(\mathrm{Gal}(L))}/\kappa(Y_L)$ has degree $|G|$. It is clear by the definition of w_{X_L/Y_L} that $\kappa(X_L)$ is contained in $\kappa(X_{\bar{\mathbb{Q}}})^{w_{X_L/Y_L}(\mathrm{Gal}(L))}$. Since $\kappa(X_L)$ also has degree $|G|$ over $\kappa(Y_L)$ it follows that $[\kappa(X_{\bar{\mathbb{Q}}})^{s(\mathrm{Gal}(L))} : \kappa(X_L)] = 1$, and they are equal. In other words you can recover the mere-cover model $X_L \to Y_L$ from its induced section. This concludes the proof of Claim (1) of the lemma.

It remains to prove Claim (2) of this lemma, i.e. that given a mere cover model $X_L \to Y_L$ the group $w_{X_L/Y_L}(\mathrm{Gal}(L))$ commutes with G if and only if $X_L \to Y_L$ is Galois. As we have seen above $\kappa(X_L)$ is equal to $\kappa(X_{\bar{\mathbb{Q}}})^{w_{X_L/Y_L}(\mathrm{Gal}(L))}$. Therefore, by Galois Theory, the cover $X_L \to Y_L$ is Galois exactly when $w_{X_L/Y_L}(\mathrm{Gal}(L))$ is normal in $\mathrm{Gal}(\kappa(X_{\bar{\mathbb{Q}}})/\kappa(Y_L))$. Since $\mathrm{Gal}(\kappa(X_{\bar{\mathbb{Q}}})/\kappa(Y_L))$ is the semi-direct product of G and $\mathrm{Gal}(\kappa(X_{\bar{\mathbb{Q}}})/\kappa(Y_L))$, this is equivalent to $w_{X_L/Y_L}(\mathrm{Gal}(L))$ commuting with G. □

Remark 3.2. The construction of α is functorial in the following sense. Let E be an overfield of L that is contained in $\bar{\mathbb{Q}}$, and let Y_E be $Y_L \times_L E$. Let Ω_E be the set of mere cover models $X_E \to Y_E$ of $X_{\bar{\mathbb{Q}}} \to Y_{\bar{\mathbb{Q}}}$ lying above Y_E. Let α' be the bijection between Ω_E and $\mathrm{Sec}(g)$ where

$g : \mathrm{Gal}(\kappa(X_{\bar{\mathbb{Q}}})/\kappa(Y_E)) \twoheadrightarrow \mathrm{Gal}(E)$ is the composition of the quotient map $\mathrm{Gal}(\kappa(X_{\bar{\mathbb{Q}}})/\kappa(Y_E)) \twoheadrightarrow \mathrm{Gal}(\kappa(Y_{\bar{\mathbb{Q}}})/\kappa(Y_E))$ with the isomorphism $\mathrm{Gal}(\kappa(Y_{\bar{\mathbb{Q}}})/\kappa(Y_E)) \xrightarrow{\sim} \mathrm{Gal}(E)$. Then $\alpha'(X_L \times_L E \to Y_E)$ is the restriction of $\alpha(X_L \to Y_L)$ to $\mathrm{Gal}(E)$.

4. Minimal Fields of Definition of a Given Model

The main theorem (Theorem 4.3) of this section states that every mere cover model of a G-Galois branched cover has a unique minimal field of definition that makes it Galois, and explores the special properties of this field. This result is somewhat surprising, since it is well known that if you do not fix the mere cover model there may not be a unique minimal field of definition for the automorphisms. (See Remark 4.4 for further discussion.)

In order to prove Theorem 4.3 we require a group-theoretic lemma (Lemma 4.2).

Notation 4.1. Let g and h be elements in a group G. We use the notation ${}^h g$ to mean the conjugation hgh^{-1}.

Lemma 4.2. *Let J and M be groups, and let I be a semi-direct product $J \rtimes M$. Let N be $M \cap C_I(J)$, where $C_I(J)$ is the centralizer of J in I. Then the following hold:*

1. *N is normal in I.*
2. *Let $\gamma : M/N \to \mathrm{Aut}(J)$ be defined by taking mN to the automorphism $j \mapsto {}^m j$. Then γ is well defined, and injective.*
3. *I/N is isomorphic to the semi-direct product $J \rtimes_\gamma (M/N)$.*

Proof. Since J is normal in I, it follows that so is $C_I(J)$. Therefore N is normal in M. In order to show that N is normal in I it suffices to prove for every n in N, j in J, and m in M that ${}^{jm}n$ is in N. Since N is normal in M, ${}^m n$ is an element of N. Since J commutes with N it follows that ${}^{jm}n = {}^j({}^m n) = {}^m n$. It is now clear that ${}^{jm}n$ is in N, and therefore (1) is proven.

The homomorphism γ is well defined because N commutes with J. It remains to show that γ is injective. Indeed if $\gamma(mN) = id$ then for every $j \in J$, we have ${}^m j = j$. Therefore m commutes with J. Since m is also in M, we conclude that it is in N. Therefore $mN = N$. This proves (2).

It is now an easy verification that the map $I = J \rtimes M \to J \rtimes_\gamma (M/N)$ taking jm, where $j \in J$ and $m \in M$, to (j, mN) is a well-defined homomorphism with kernel N, proving (3). □

We are now ready for the main theorem of this section:

Theorem 4.3. *Let G be a finite group, and let $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ be a G-Galois branched cover that descends as a mere cover to a number field L. Let $X_L \to \mathbb{P}^1_L$ be a model of it over L, and let $\mathcal{A}$ be the set of all overfields E of L such that $X_L \times_L E \to \mathbb{P}^1_E$ is Galois. Then there is a field E in $\mathcal{A}$ that is contained in all of the other fields in $\mathcal{A}$, and it satisfies the following properties:*

1. *The field extension E/L is Galois, with Galois group isomorphic to a subgroup H of $\mathrm{Aut}(G)$.*
2. *For every G-Galois field extension F/E coming from specializing the G-Galois branched cover $X_L \times_L E \to \mathbb{P}^1_E$ at an E-rational point, the field extension F/L is Galois with Galois group isomorphic to $G \rtimes H$ (where $\mathrm{Gal}(F/E) \cong G$ is the obvious subgroup of $G \rtimes H$, and where the action of H on G is given by the embedding of H in $\mathrm{Aut}(G)$).*

Proof. Let $L(x)$ be the function field of $\mathbb{P}^1_L$, where x is a transcendental element. By Lemma 2.4 in [1], $\kappa(X_{\bar{\mathbb{Q}}})$ is Galois over $L(x)$. Let $s : \mathrm{Gal}(L) \to \mathrm{Gal}(\kappa(X_{\bar{\mathbb{Q}}})/L(x))$ be the section corresponding to $X_L \to \mathbb{P}^1_L$ via the bijection α from Lemma 3.1.

Let V be the intersection of $s(\mathrm{Gal}(L))$ with the centralizer of G in $\mathrm{Gal}(\kappa(X_{\bar{\mathbb{Q}}})/L(x))$. Applying Lemma 4.2 with G in the role of J, $s(\mathrm{Gal}(L))$ in the role of M, V in the role of N,

and $\mathrm{Gal}(\kappa(X_{\bar{\mathbb{Q}}})/L(x))$ in the role of I, we see that V is normal in $\mathrm{Gal}(\kappa(X_{\bar{\mathbb{Q}}})/L(x))$, and that $\mathrm{Gal}(\kappa(X_{\bar{\mathbb{Q}}})/L(x))/V$ is isomorphic to a semi direct product of G with a subgroup of $\mathrm{Aut}(G)$. In particular, the group V is has finite index in $\mathrm{Gal}(\kappa(X_{\bar{\mathbb{Q}}})/L(x))$, and therefore the compositum GV is an open subgroup of $\mathrm{Gal}(\kappa(X_{\bar{\mathbb{Q}}})/L(x))$ containing G. Therefore there exists a finite field extension E of L, contained in $\bar{\mathbb{Q}}$, such that the fixed subfield of $\kappa(X_{\bar{\mathbb{Q}}})$ by GV is equal to $E(x)$. Note that $\kappa(X_L \times_L E)$ is the fixed subfield of $\kappa(X_{\bar{\mathbb{Q}}})$ by V.

We first show that E is an element of $\mathcal{A}$, and in fact the least element (i.e. $\forall E' \in \mathcal{A}\ \ E \subseteq E'$). By Lemma 3.1 and Remark 3.2, the map $X_L \times_L E \to \mathbb{P}^1_E$ is Galois because the image of the restriction of s to $\mathrm{Gal}(E)$ commutes with G. If E' is another element of $\mathcal{A}$, then again by Lemma 3.1 and Remark 3.2 the image of the restriction of s to $\mathrm{Gal}(E')$ commutes with G. But this implies that $\mathrm{Gal}(\kappa(X_{\bar{L}})/E'(x))$ is contained in GV. This proves that E is the least element in $\mathcal{A}$.

The group $\mathrm{Gal}(E/L) \cong \mathrm{Gal}(E(x)/L(x))$ is isomorphic $s(\mathrm{Gal}(L))/V$ by the second isomorphism theorem. It follows from the above that $\mathrm{Gal}(E/L)$ embeds into $\mathrm{Aut}(G)$. This proves Claim (1) of Theorem 4.3.

Claim (3) of Lemma 4.2, applied to our situation as above, implies that the field extension $\kappa(X_L \times_L E)/L$ is Galois with Galois group isomorphic to $G \rtimes H$ (where the action of H on G is given by the embedding of H in $\mathrm{Aut}(G)$); and that furthermore, we have $\kappa(X_L \times_L E)^G = E(x)$. Claim (2) in Theorem 4.3 is now proven by specializing.

□

Remark 4.4. Let $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ be a G-Galois branched cover with field of moduli M. Recall that the field M is the intersection of all of the fields of definition of $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ as a G-Galois branched cover, but is not necessarily one itself. However, since M contains the field of moduli of $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ as a mere cover, it is a field of definition as a mere cover. (See Section 2.) In light of Theorem 4.3, one can explain the failure of M to be a field of definition as a G-Galois branched cover as the combination of two factors:

(1) Theorem 4.3 gives a unique minimal field of definition as a G-Galois branched cover for any particular mere cover model $X_M \to \mathbb{P}^1_M$. However each model might give a different minimal field of definition. Therefore the non-uniqueness of a model of $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ over M contributes to the plurality of the minimal fields of definition.
(2) If L is an overfield of M, then there may be a mere cover model of $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ over L that does not descend to a mere cover model over M.

This theorem has a number of noteworthy corollaries.

Corollary 4.5. *Let G be a finite group, and let $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ be a G-Galois branched cover. Then the following hold:*

(1) *Assume $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ descends as a mere cover to a number field L (i.e., L contains the field of moduli as a mere cover). Then there exists a field of definition for $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ as a G-Galois branched cover that is Galois over L with Galois group a subgroup of $\mathrm{Aut}(G)$. In particular this holds when L is the field of moduli of $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ as a G-Galois branched cover.*
(2) *Assume $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ descends as a mere cover to a number field L. Then there exists a subgroup $H \leq \mathrm{Aut}(G)$ such that $G \rtimes H$ is realizable as a Galois group over L.*
(3) *Let F be the field of moduli of $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ as a mere cover, and let M be the field of moduli of $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ as a G-Galois branched cover. Then M is Galois over F with Galois group a subquotient of $\mathrm{Aut}(G)$.*

Proof. Claims (1) and (2) follow immediately from Theorem 4.3. In light of Theorem 4.3, in order to prove Claim (3) it suffices to show that M is Galois over F. Recall that M is the intersection of all of the fields of definition as a G-Galois branched cover. It therefore suffices to prove that for every field of definition L of $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ as a G-Galois branched cover, and for every σ in $\mathrm{Gal}(\bar{\mathbb{Q}}/F)$, the field σL is also a field of definition as a G-Galois branched cover. Let $X_L \to \mathbb{P}^1_L$ be an L-model as a G-Galois branched cover, and let $X_{\sigma L} \to \mathbb{P}^1_{\sigma L}$ be its twist by σ. This cover is clearly Galois. Furthermore, note that $X_{\sigma L} \to \mathbb{P}^1_{\sigma L}$ is a mere cover model over σL of the cover $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ after it has been twisted by σ. By the definition of F, the cover resulting from twisting $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ by σ is isomorphic to $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ as a mere cover. Therefore σL is a field of definition of $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ as a mere cover, and $X_{\sigma L} \to \mathbb{P}^1_{\sigma L}$ is a mere cover model of this cover that is Galois. In other words, the field σL is field of definition of $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ as a G-Galois branched cover, which is what we wanted to prove. □

Remark 4.6. Note that Claim (3) in Corollary 4.5 implies that there exists a subgroup $H \leq \mathrm{Aut}(G)$ such that $G \rtimes H$ is a Galois group over L without proving it is realizable regularly (i.e. as the Galois group of a regular extension of $L(x)$).

5. Adjoining Roots of Unity to a Field of Moduli to get a Field of Definition

While Theorem 4.3 describes a general relationship between the field of moduli and fields of definition, the main theorem of this section (Theorem 5.1) describes the existence of a particular field of definition (infinite over the field of moduli) with special properties.

Let G be a finite group, and let $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ be a G-Galois branched cover. As noted in Section 2, its field of moduli M as a G-Galois branched cover may not be a field of definition as a G-Galois branched cover. However, Coombes and Harbater ([3]) have proven that the field $\cup_n M(\zeta_n)$ resulting from adjoining all of the roots of unity to M *is* a field of definition. (Here ζ_n is defined to be $e^{\frac{2\pi i}{n}}$.) The following is a strengthening of this result.

Theorem 5.1. *In the situation above, the field $\cup_{\{n|\exists m: n||Z(G)|^m\}} M(\zeta_n)$ is a field of definition. In particular, there exists a field of definition (finite over $\mathbb{Q}$) that is ramified over the field of moduli M only over the primes that divide $|Z(G)|$.*

Proof. If G is centerless, then the cover is defined over its field of moduli ([3]) and therefore the theorem follows. Otherwise $\cup_{\{n|\exists m: n||Z(G)|^m\}} M(\zeta_n)$ satisfies the hypotheses of Proposition 9 in Chapter II of [12]. We conclude that $\mathrm{cd}_p(\cup_{\{n|\exists m: n||Z(G)|^m\}} M(\zeta_n)) \leq 1$ for every prime p that divides $|Z(G)|$. This implies that $H^2(\cup_{\{n|\exists m: n||Z(G)|^m\}} M(\zeta_n), Z(G))$ is trivial. As the obstruction for this field to be a field of definition lies in this group ([6]), we are done. □

Combining Theorem 5.1 with results that I have proven in [10], we get the following corollaries.

Corollary 5.2. *Let G be a finite group. Then the following hold:*

1. *For every positive integer r there is a set $T = \{a_1, ..., a_r\}$ of closed points of $\mathbb{P}^1_{\bar{\mathbb{Q}}}$, such that every G-Galois branched cover of $\mathbb{P}^1_{\bar{\mathbb{Q}}}$ that is ramified only over T, has a field of definition that is unramified (over $\mathbb{Q}$) outside of the primes dividing $|G|$.*
2. *For every positive integer r, and for every finite set S of rational primes that don't divide $|G|$, there is a choice of $\mathbb{Q}$-rational points $T = \{a_1, ..., a_r\}$ such that every G-Galois étale cover of $\mathbb{P}^1_{\bar{\mathbb{Q}}} \smallsetminus T$ has a field of definition that is unramified (over $\mathbb{Q}$) over the primes of S.*
3. *There is an extension of number fields $\mathbb{Q} \subset E \subset F$ such that F/E is G-Galois, and $E/\mathbb{Q}$ ramifies only over those primes that divide $|G|$.*

Proof. Claims (1) and (2) of the corollary are straightforward from Theorems 9.1 and 9.6 of [10] respectively, together with Theorem 5.1. Claim (3) follows from Claim (1) by specializing. □

References

[1] Beckmann, Sybilla. "Galois groups of fields of definition of solvable branched coverings," Compositio Math. 66 (1988), no. 2, 121-144.

[2] Belyi, G.V. "On Galois extensions of a maximal cyclotomic field," (Russian) Izv. Akad. Nauk SSSR Ser. Mat. 43 (1979), no. 2, 267-276, 479.

[3] Coombes, Kevin; Harbater, David. "Hurwitz families and arithmetic Galois groups," Duke Math J., 52 (1985), 821-839.

[4] Dèbes, Pierre. "Algebraic covers: field of moduli versus field of definition," (English, French summary) Ann. Sci. cole Norm. Sup. (4) 30 (1997), no. 3, 303-338.

[5] Dèbes, Pierre. "Covers of $\mathbb{P}^1$ over the p-adics." Recent developments in the inverse Galois problem (Seattle, WA, 1993), 217-238, Contemp. Math., 186 (1995), Amer. Math. Soc., Providence, RI.

[6] Dèbes, Pierre. "Descent theory for algebraic covers," Arithmetic fundamental groups and noncommutative algebra (Berkeley, CA, 1999), 3-25, Proc. Sympos. Pure Math., 70 (2002), Amer. Math. Soc., Providence, RI.

[7] Dèbes, Pierre. "Groupes de Galois sur K(T)," (French) Sm. Thor. Nombres Bordeaux (2) 2 (1990), no. 2, 229243.

[8] Fried, Michael; Jarden, Moshe. "Field Arithmetic," third edition, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], 11. Springer-Verlag, Berlin (2008).

[9] Grothendieck, Alexander. "Séminaire de Géométrie Algébrique," mimeographed notes (1960-61), I.H.E.S., Paris, no. 1.

[10] Hasson, Hilaf. "The prime-to-p part of étale fundamental groups of curves," 2012 preprint, available at arXiv:1209.3693.

[11] Matzat, B. Heinrich. "Konstruktion von Zahl- und Funktionenkörpern mit vorgegebener Galoisgruppe," J. reine u. angew. Math. 349 (1984), 179-220.

[12] Serre, Jean-Pierre. "Cohomologie Galoisienne" fifth edition, Lecture Notes in Mathematics (1994), no. 5, Springer-Verlag, Berlin.

[13] Wewers, Stefan. "Field of moduli and field of definition of Galois covers," Arithmetic Fundamental Groups and Noncommutative Algebra (1999), 221-245, edited by M. D. Fried and Y. Ihara, Proc. Sympos. Pure Math. 70, Amer. Math. Soc., Providence, RI, 2002.

Current author information:

Hilaf Hasson: Department of Mathematics, Pennsylvania State University, State College, PA 16802, USA

email: `hilafhasson@gmail.com`